

# Evaluating Data Center High-Availability Service Delivery

A FORTRUST White Paper

June 2008

**FORTRUST™**  
*premium data center services*

*When companies evaluate potential data center service providers, they normally compare them using some kind of criteria or checklist. However, many such evaluations fail to sufficiently evaluate the breadth and depth of detail necessary to make a well informed decision.*

*This white paper examines several key criteria as they relate to high-availability service delivery. Specifically, this paper examines the importance of factors such as operational processes and service assurance, combined with maintenance and lifecycle strategies.*

*If you have any questions about this white paper or FORTRUST in general, please don't hesitate to contact your FORTRUST representative for additional information.*

## Introduction

The search for the right data center services provider to support colocation or hosting requirements is not an easy one. Companies rely on data center services providers to minimize the chances of downtime occurring for critical applications and make it easier to manage their IT infrastructure requirements. Therefore, they need to be able to make informed decisions when choosing a data center in which to entrust and house their business-critical applications. And while the choices are plentiful, choosing the wrong data center services provider can be a costly mistake.

That's why companies spend considerable time and energy selecting their data centers. They conduct research, tour data centers, submit requests for information, review proposals and check references. The key is to ask the correct questions. By asking their potential data center service providers questions, they uncover important information about the facility, network access, operations and service quality. Making the right decision, it seems, often depends on asking the right questions. But how do you know if you're asking questions that truly help you make an informed decision?

As a world-class high-availability data center services provider, FORTRUST has worked closely with companies of all sizes to make sure they're making the right choices for their businesses. In doing so, FORTURST has answered a lot of questions to help companies make decisions. Leveraging this experience, FORTRUST has compiled a list of questions companies should be asking—but often don't. This list is far from exhaustive, and is not intended to be applicable in every situation or to every data center services provider; instead, it is designed to help companies make the right decisions for their businesses.

In this white paper, you'll read about some additional criteria companies should evaluate when choosing their data center. At the end of the paper is a worksheet where you'll find a list of evaluation questions. These questions may help you gather the important information you need to make a rational and well-informed decision about your data center services provider.

The information provided in this document is intended only to be a starting point. For more information, we suggest you examine the excellent work performed by organizations such as the Uptime Institute and the American Society of Heating, Refrigerating and Air-Conditioning Engineers (ASHRAE) and others on the subjects of reliability, availability, uptime and critical systems infrastructure design.

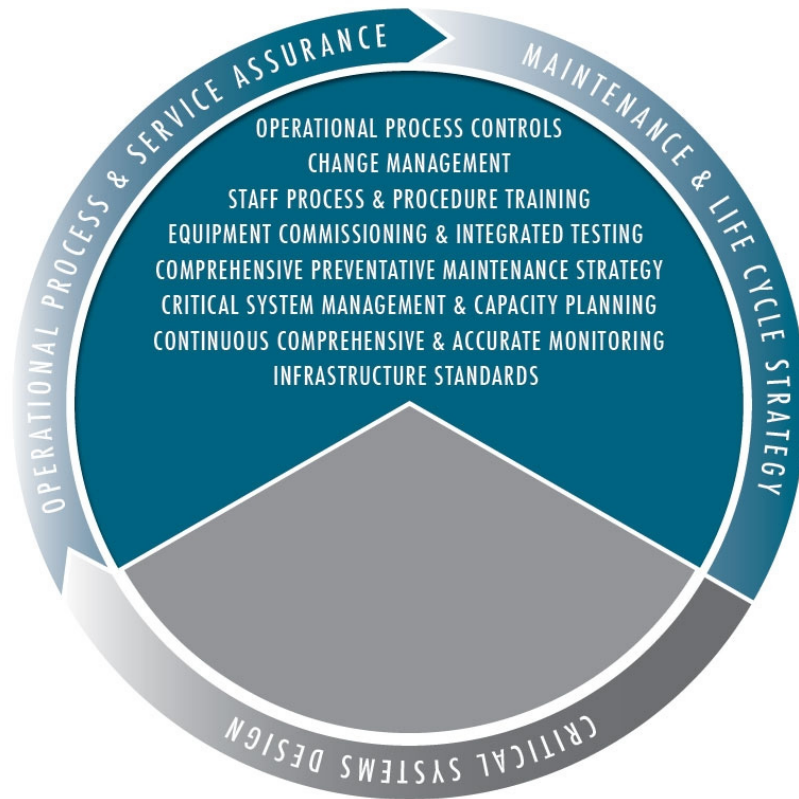
## A Closer Look at Reliability and High-Availability Service Delivery

Each company has unique requirements, and look for different attributes from its data center services provider. Most companies, however, are looking for a provider that offers reliability and high availability. But not all data centers are alike.

In many cases, companies examine the facility's critical systems infrastructure, location, building characteristics, business stability, data center environment, connectivity, and physical security. While all of these attributes are important when evaluating data centers, companies should also focus on factors that play an important role in ensuring high-availability service delivery, such as each provider's operational processes, service assurance policies and maintenance and lifecycle strategies.

Even though data centers are designed to provide different levels of reliability, high-availability service delivery is not achieved by design alone. While reliability does stem from a combination of many factors starting with design, other practices that lend themselves to high-availability service delivery include:

- Operational process controls for the critical systems infrastructure, including change management and staff training on processes and procedures that mitigate or eliminate errors and ensure high service levels
- Equipment commissioning and integrated systems testing
- A comprehensive preventive and predictive maintenance strategy combined with meaningful testing and trend analysis and a commitment to replacing or repairing equipment before it can fail
- Critical systems infrastructure management and capacity planning
- A continuous, comprehensive and accurate monitoring and data collection system for all critical and essential systems, combined with a notification, escalation and resolution process
- The use of infrastructure standards for the uniform identification and management of equipment throughout the electrical, heating, ventilation and air conditioning (HVAC), and connectivity systems.



**Diagram 2.1 High Availability Service Delivery Model**  
 (Source: FORTRUST)

The concepts of reliability and high availability services delivery are facilitated through an operational mindset in which attention to detail, process discipline and procedural compliance need to emanate from every aspect of the provider’s approach to operations and service delivery.

# Key Data Center Selection Criteria

## Location and Facility

One of the first factors you should consider when evaluating data center services providers is the facility and its location. While it is important to choose a data center that's easy for your support staff to access, the location of the data center is also significant for a number of other reasons. One of these is the utility grid. In order to minimize the chances of disruptions in your data center's power supply, you want to look for a data center fed by a reliable utility grid. Even though data centers in newer areas may be less likely to be connected to a well-established power supply, you can best determine the reliability of the grid by contacting the local utility. Most will provide information and reports on their performance. The data center services provider should also be able to supply this information.

Although utility outages do not necessarily translate to data center outages or even critical equipment downtime due to the use of uninterruptible power supplies (UPSs) and backup generators, unstable utility power causes unnecessary wear and tear on UPS batteries and associated equipment, and could also be a sign of capacity and quality issues.

Construction also can affect the utility grid. So whether the data center is located close to residential areas with new construction or in a zone undergoing revitalization, these factors can potentially impact the quality of the facility's power supply and, potentially, your servers' uptime.

Along with looking for potential problems with the utility grid, you also should investigate whether the data center is in a zone or region that is rated as being at risk of experiencing natural disasters. Earthquakes, hurricanes, floods and tornadoes can all damage—if not destroy—even the most sturdily built data center.

Location is important to consider in terms of climate as well. If the data center you're evaluating is in a cold-weather region, check to see if it is located on an emergency route. Because these roads are normally cleared during snowstorms, it is more likely that your data center will be staffed and accepting deliveries (such as backup fuel supplies) and will be easier for you to access in inclement weather. Data centers not positioned on emergency routes may not be so lucky during the next blizzard.

Another factor to consider is the facility's construction. Some data centers were built specifically to be data centers, while others were renovated shells or existing structures that eventually became data centers. Because renovated shells or existing structures may be missing key structural elements, they may be more susceptible to storms and problems with ongoing sustainability and may lack the necessary physical security measures. Inquiring about the facility's construction can provide a lot of good information on its structural integrity.

The facility's proximity to other resources is also a factor worth looking at. Obviously, facilities that are located closer to the local fire department will benefit from swifter response during emergencies. On the other hand, proximity to airports may present potential risks by putting the facility under the flight path of arriving and departing airplanes.

## Business Stability

Business stability is also an important factor to consider when selecting a data center services provider. Business stability is important because you don't want to be forced to relocate your equipment should the data center services provider suddenly go out of business.

## Data Center (Raised Floor) Environment

Data centers often are built using raised floors, which provide a plenum for cooling. Data center experts recommend a minimum of 18 inches above the sub floor for raised floors, but 24 inches and even 36 inches are becoming the desired height. The reason for the higher raised floors is clear: the more space there is for air to flow, the easier it will be to cool the data center. That's why newer data center designs often feature cabling that runs above the equipment racks or cabinets, rather than below the raised floors. Cabling, conduit, raceways and other items that are placed underneath the raised floors take up valuable space used for cooling that can further impede the flow of air and potentially cause variations in plenum pressure, hot spots, and potentially cleanliness issues.

Higher ceilings also aid in air flow and help with cooling. Ceilings should be high enough to provide enough room for cabling, while allowing hot air generated by equipment to rise and be circulated back to the HVAC system.

When evaluating data centers with raised floors, it is also important to look at whether the raised floor is over a concrete slab, providing stability and support for heavy equipment. Additional stability is offered by raised floors that are attached to the concrete slab and by equipment cabinets or racks that are anchored to the slab rather than simply sitting on the raised-floor tiles.

When touring prospective data centers, you should also determine how much space is available for new equipment—and how it can be configured. Having ready-to-use space and a variety of set-up options to choose from, such as private cabinets, cages with racks and private rooms or vaults, is important because it not only means the data center can meet your needs now, but also can easily meet your needs in the future should you wish to expand.

Space considerations can go far beyond the amount of available raised-floor space, however. Access to onsite office space and temporary storage space is also important. Office space can be used in the event of a disaster or when you are at the data center

working on equipment, while secure onsite storage space lets you have equipment shipped directly to the data center without having to worry about having your employees on hand to receive it.

## Access and Connectivity

When evaluating your options, it is critical to understand the connectivity and access options that each data center services provider offers. Because of this, many companies ask questions associated with the carriers present in the facility, whether or not they have fiber in the facility and at what capacities.

Multiple and diverse fiber runs offered by different providers also offer an additional benefit: redundancy. For customers that choose to take advantage of such an option, this means that should one provider's backbone fail, traffic can automatically be switched over to another provider's network. Also, to optimize physical diversity, the data center should bring fiber into its facility from at least two separate locations. By doing so, the data center services provider ensures traffic will continue to flow even if all the conduits or fiber coming through one of the entrance points is cut or damaged.

Carrier neutrality is also an important concern. The term carrier neutral should not only mean that the customer can use any access service provider that it wants, but also that the data center services provider makes it as easy as possible for its customers to do so. To support true carrier neutrality, data center services providers normally will have fiber provided by several different carriers installed in the facility, and will help their customers gain access to any other carrier they choose that may not already be present in the facility. By choosing a truly carrier-neutral provider, you're able to use the carrier (or a combination of carriers) that makes the most sense for your business.

## Physical Security

Physical security is just as important as virtual security when it comes to protecting data housed in a data center. While many data center services providers put some security measures into place, security approaches can differ greatly from one facility to the next. More rigorous approaches will rely on a multi-layered security strategy that provides a wide variety of defenses that make it more difficult for unauthorized access to occur.

One of the best ways to help secure a facility is to make it practically disappear by keeping a low profile. Unfortunately, data center services providers that post signage above their facilities can draw attention to themselves—and their customers. In addition, data center services providers that list their customers on their marketing materials run the risk of exposing those customers to potential risks by advertising where their servers and equipment are housed.

## Operational Process Controls and Service Assurance, Maintenance and Lifecycle Strategies

How a data center services provider handles its operations can greatly impact your experience colocating your equipment at its facility. One important factor to consider is the provider's processes associated with maintenance and ongoing day-to-day operations surrounding service-assurance controls.

Process control and documentation of processes are critical, since many unplanned downtime incidents are the result of human error. That's why documented, validated and repeatable processes are important—the more procedures and processes are documented, the more likely it is that they will be followed, and the less likely it is that human error will cause a disruption in service. Just as important is how well these procedures are disseminated—the data center services provider must provide adequate training on their usage and be able to ensure that the procedures are followed. In other words, it is critical that the provider does a good job of implementing procedural compliance throughout its operations organization.

Another operational consideration to take into account is service-level agreements (SLAs). While many people ask about availability SLAs, far fewer inquire about the data center services provider's temperature and humidity SLAs. These are important for minimizing the chances of equipment failure and downtime by ensuring the data center's temperature and relative humidity fall within an acceptable range and are properly delivered in sufficient capacity to the cooling intakes of the customers' servers and associated equipment. It is also necessary to understand in detail how these SLAs are monitored and measured.

In addition, the commissioning of equipment and its initial validation or integrated systems testing are important. These tasks are normally accomplished at the completion of initial construction or additional space and infrastructure expansions, and may be conducted by a third party in order to provide a comprehensive evaluation of the independent systems and components of the electrical, HVAC and critical systems infrastructure.

Detailed commissioning should also include an extensive integrated systems test that provides information and data on how the systems react together in different load and potential failure scenarios. It will also test to validate design capacities, redundancies, reliabilities and the sequencing of building management systems in order to determine whether or not the systems are able to produce the desired results as designed and constructed.

Regular preventive and predictive maintenance combined with a lifecycle strategy is critical to ensuring the availability and reliability of equipment and systems. And because maintenance procedures and processes can differ dramatically from one data center services provider to the next, it is important to closely evaluate each provider's procedures to determine if the provider has them and, if so, what they are and who performs the work.

## Critical Systems Infrastructure Management and Capacity Planning

There are five key areas to the critical systems infrastructure that you may want to consider when choosing a data center services provider:

- Critical equipment
- Critical and essential electrical systems
- Critical HVAC systems
- Fire and safety equipment
- Critical systems and equipment monitoring

### Critical Equipment

The performance of a data center's critical equipment, such as UPS devices, generators and chillers, is affected by several factors: the age of the equipment, the process by which the equipment is selected and redundancy. (It is also impacted by how and at what intervals or periodicities it is maintained, monitored, inspected and tested; this is discussed in greater detail in the previous section about operational process controls.)

- **Age.** All too often, data center services providers continue to rely on equipment that has exceeded its useful life. This can be risky, because as a piece of equipment gets older, the chances of it failing increase. Newer equipment, on the other hand, normally has less risk of failure, so that there are fewer chances of downtime occurring.
- **Selection process.** As data center services providers replace or buy new equipment, they must make important decisions. Some providers select equipment for the facility based on the lowest bid they receive, while others take a best-in-class approach. By using best-in-class equipment, providers are protecting their customers' needs rather than their bottom line. In addition, performance and mean time before failure (MTBF) should be considered when making critical equipment choices.
- **Redundancy.** Formulas such as N+1 are often used to describe the level of redundancy data center services providers rely on to back up critical components. They describe a configuration in which necessary components, referred to as N, have a backup component. Done correctly, this type of redundancy helps reduce the chances of equipment failure affecting data center customers, while enabling standard routine maintenance to be performed without impacting customers.

### Critical and Essential Electrical Systems

The quality of the electrical distribution systems can make or break a data center services provider's performance and reliability. When evaluating providers, it is important to look at the power available to the data center. It is important to understand the number of utility feeds received by the facility, the capacity available on each feed and the voltage received from the utility service.

But just as important is the provider's plan for handling potential power outages. Data center services providers should have several emergency backup generators installed and ready to go at all times. Since generators are powered by fuel—usually diesel—it is a good idea to find out how long each generator can run at full load, how much additional fuel the provider keeps on site and how it plans on getting more fuel in the event of a longer utility outage.

While generators are vital to providing power during outages, they do not work instantaneously. That's why UPS devices are important, since they will provide continuous power in the event the main power is disrupted. They can also help alleviate problems with the power such as voltage sags or spikes and keep them from damaging your equipment.

### **Critical HVAC Systems**

Keeping data center space cool is a critical component of any provider's operations. When evaluating data center services providers, be sure to ask for a detailed description of the facility's cooling systems its capacity and redundancy. Additionally, you should investigate the cooling system's capacity and how the provider controls temperature and humidity in the raised-floor areas.

### **Fire and Safety Equipment**

Being able to respond quickly to potential fires is also critical in a data center. The providers you are considering should not only have smoke detection and fire suppression systems in place, but also early warning systems that sample the air for smoke, allowing the provider to quickly respond to potential problems. In addition, the provider should make portable extinguishers readily available and should have them regularly tested.

### **Critical Systems and Equipment Monitoring**

Critical systems require constant, accurate and reliable monitoring. In a highly reliable environment that is focused on the delivery of high-availability services, the monitoring systems are just as important as the equipment being monitored for a variety of reasons. Monitoring systems will alert personnel quickly to changes or issues often before they become critical or may possibly impact availability. Also, properly configured monitoring systems can be used to track trends that indicate adherence to SLAs and can be used for systems and performance analysis and for immediate notification of potential issues.

## Conclusion

Every data center services provider is unique. Some offer greater reliability and security than others, but these qualities are not always easy to determine. That is why selecting a data center can be such a long and arduous process. However, by asking the right questions, you have a better chance of ensuring that you are making the right decision.

## Learn More

FORTRUST is the leading high-availability data center in the Rocky Mountain region for businesses seeking world-class colocation and data center services. To learn more, visit [www.FortrustDataCenter.com](http://www.FortrustDataCenter.com).

## Appendix A: Worksheet

Consider using the following questions when evaluating data center services providers. More information about each of the subject areas can be found in the body of the white paper.

Please note: A lot of the questions contained within this worksheet will lead to a variety of different answers, many of which are neither right nor wrong. It is up to you to determine whether the questions or the subsequent responses address your organization's requirements for its future data center services provider.

### Location and Facility

- Is there a lot of construction going on near the data center?
- Does the data center have access to more than one utility grid or separate feeders from different substations?
- Is the data center located on an emergency route?
- What is the zoning classification?
- Is the data center located in an area that puts it at risk of earthquakes, hurricanes, floods, tornados or wildfires? If yes:
  - How would you rate that risk?
- What are the sources of your data about natural disaster risks associated with the geographic location of the data center?
- What is the history of storms, floods, tornados, hurricanes or other natural disasters at that location?
- Where is the facility located in relation to the 100-year floodplain?
- What is the maximum predicted flood elevation?
- What is the probability of seismic activity?
- In what seismic zone is the facility located?
- Are there seismic enhancements to the facility's construction or within the critical systems infrastructure? If yes:
  - Provide a detailed description of the facility's seismic enhancements.
- Is a lightning protection system in place for the entire facility?
- What are the company's contingency procedures for other events or potential risks associated with the data center's location? Are these procedures documented?
- How old is the building in which the data center is housed?
- Was the facility built as a data center or is it a converted shell or other type of building? If yes:
  - What was its original purpose?
- How is the facility constructed? (For example, what were the exterior walls made out of and what are the interior wall fire ratings?)
- What materials were used in the roof construction?
- Are there windows located in the data center (raised-floor areas)?
- If there are windows in the facility but not necessarily in the raised-floor areas, are they hardened or treated from a physical security standpoint?

- Is the facility reinforced in any way? If yes:
  - Provide a detailed description of the facility reinforcements.
- Can the facility's construction documentation and as-built drawings be made available for review?
- How close is the nearest fire department or first responders?
- Is the facility near or in the flight path of an airport?
- How are potential risks from the local area mitigated?
- Is there a hazmat spill procedure that we can review?
- What are the operational profile and contingency plan in case the facility and surrounding area must be evacuated?

## Business Stability

- Is the company privately or publicly held? If privately held:
  - Do you have financial information you could provide that would indicate the health of the company?
- How long has the business been operating in the data center business?
- Is the business fully funded for growth?
- Are the data center and its equipment and facility wholly owned and operated by the business?
- Are there any major components of the electrical or HVAC system that are owned and therefore maintained by someone other than the owner/operator?
- Are high-availability data center services the primary focus from a services standpoint?
- Is there a disaster recovery and business continuity plan in place?

## Data Center (Raised Floor) Environment

- What is the electrical and cooling density in watts per square foot and/or BTUs per square foot?
- Are there restrictions or limits on power and subsequent cooling capabilities to an individual cabinet or rack? If yes:
  - What are those limits?
- What is the height of your raised floors?
- Do you run cabling under the floors? If yes:
  - How do you keep cabling from restricting airflow, which can create potential pressure differences?
  - What are the cleanliness standards and how are they achieved?
  - What is contained under the raised floor?
- At what pressure is the raised-floor plenum maintained?
- What is the designed or desired cubic feet per minute (CFM) of air flow in the delivery aisle per tile? How is this monitored?
- Is the entire data center space built on the ground floor?
- Is your raised floor attached to the concrete slab?
- Do cabinets or racks sit un-anchored on raised floors? If no:

- Are they anchored only to the raised floor or are they anchored to the concrete slab or floor?
- What is the load capacity of your raised floor in concentrated load and uniform load?
- Is your raised floor grounded?
- What are your minimum ceilings heights (measured from the top of the raised floor)?
- Is the ceiling over the raised floor susceptible to radiant heat changes and condensation issues? If yes:
  - How do you counteract this?
  - Does water from a source other than an extinguishing system run over the raised-floor areas in any fashion?
- How much space do you have available in your data center? How quickly can you build out the space?
- Is there adequate space for critical components and systems infrastructure for growth and density?
- What is the ratio of raised floor space to mechanical, electrical and critical systems space?
- Do you offer customers access to onsite office space? If yes:
  - Is this permanent, temporary or a disaster recovery-type of offering?
- Under what conditions can a customer gain access to the onsite office space?
- Can we have equipment drop-shipped to the data center?
- What is your process for handling customer equipment drop-shipped to the data center?
- What is the security protocol around items being received at the location?

## Access and Connectivity

- What is the bandwidth capacity at the facility, per carrier?
- Is your data center carrier neutral? If yes:
  - How do you define the term carrier neutral?
- What carriers have installed fiber in your data center?
- How does the fiber enter the facility and how is it secured?
- Is the fiber exposed at any point inside the facility so that someone can gain access to it?
- Does the fiber enter the building in more than one location?
- Are the fiber entrances secured and separated? If yes:
  - By what manner and distance?
- Is the fiber transported in conduit? If yes:
  - Can it be accessed in the facility or is it secured?
  - Does the conduit run under the slab of the facility?
- Can I use a carrier other than the ones that already service your data center?
- Are you open to having different carriers have a presence in the data center?
- How do you allow for the use of other carriers in your facility?
- What is your policy on cross-connects?
- Do you provide a managed Internet-access solution that's over redundant and diverse carriers?

## Physical Security

- What types of physical security measures do you have in place?
- Please describe in detail your approach to physical security with respect to administrative processes for granting access to people such as customers, vendors and visitors.
- Are your access controls multi-layered? How?
- Is there around-the-clock dedicated security personnel onsite? If yes:
  - Do the security personnel have other duties assigned to them? What are these duties?
- Are all of the facility's exterior entrance and exit points monitored by cameras?
- Are exterior entrances and exit points alarmed? If yes:
  - How often are the alarms tested?
- Is power for the physical security system on a UPS?
- Is there camera monitoring throughout the data center areas? If yes:
  - How are the cameras monitored?
  - Are they monitored around the clock?
  - Are they monitored by others in addition to the assigned security personnel?
- Are the cameras recorded?
- Are there manned security checkpoints and/or traps?
- How often are security tours through the facility conducted?
- Are the windows alarmed?
- What areas are accessible via windows?
- Are the facility and windows resistant to explosions?
- Is roof access restricted, alarmed or monitored?
- Are customer areas including cabinets, cages and rooms secured in layers?
- Do you use an offsite monitoring company to provide additional layers of security?
- Do you use any forms of biometric access controls? If yes:
  - What types and in what fashion?
- Is the facility location susceptible to crimes?
- What is your procedure for items shipped to and received at the facility?
- Are the receiving areas monitored by security personnel?
- Has your data center ever experienced any security incidents?
- Who is responsible for developing your security procedures?
- Are your security procedures documented?
- How often do you have outside parties audit your security practices?
- Do you post any signs on the exterior of the facility that may indicate that it's a data center?
- Will our company's presence in the facility be advertised in any fashion?
- Do you list your customers housed in your facility anywhere, such as on your marketing materials?

## Operational Process Controls and Service Assurance, Maintenance and Lifecycle Strategies

### Processes and SLAs:

- What are your change management controls? Is there a documented process for change management?
- Do you document your maintenance and operational procedures? If yes:
  - Are the documented procedures available for review?
- Are there procedures or contingency plans for identified potential risks?
- Are revisions to your documented procedures controlled? How?
- How is staff training conducted for processes and procedures?
- What are your SLAs for electrical power availability?
- What are your SLAs for environmental availability?
- Do you have SLAs for temperature and humidity? If yes:
  - What are they?
- What are your SLAs for technical response and/or remote hands?
- Are there penalties (such as service credits) for exceeding the ranges established by the temperature and humidity SLAs? If yes:
  - Must the customer request an SLA credit if applicable or do you automatically provide the credit?
- How are your temperature and humidity SLAs measured and monitored?
- Are temperatures and humidity measured in the delivery aisles above installed computer equipment?
- Is there around-the-clock facilities staff onsite other than security or network operations staff?
- Please provide a description or matrix of your escalation procedures for all operational events and customer service delivery issues.

### Equipment commissioning and initial validation or integrated systems testing:

- Was an electrical short-circuit coordination study conducted? If yes:
  - Is it available for review?
- Were the data center facility and critical-systems infrastructure commissioned by a third party or commissioning agent? If yes:
  - Did the commissioning include an integrated systems test to validate the design capacities, redundancies and reliabilities of critical equipment in different modes of failure?
  - Are the commissioning and integrated systems test reports available for review?

### Preventive and predictive maintenance and lifecycle strategies

- How is the scheduling for your preventive and/or predictive maintenance managed? For example, is it automatically generated by a software program, do you use hard-copy scheduling or do you use an outside vendor to manage it?

- Do you keep a maintenance history for all critical equipment? If yes:
  - Can the maintenance history for a specific piece of equipment be reviewed?
- What kind of documented preventive and predictive maintenance procedures do you have in place?
- Are maintenance schedules and equipment history records available for review?
- How often do you conduct your maintenance activities?
- Do you handle maintenance in-house or is it outsourced? If maintenance is outsourced:
  - Who does the work and at what intervals?
- What types of maintenance activities are performed during the maintenance windows?
- What are the frequencies of facility-related (electrical or HVAC) maintenance windows?
  - Does this maintenance work affect redundant circuits to computer racks or cabinets?
- Can you provide a list and description of all the facility-related (electrical or HVAC) maintenance windows for the prior year?
- Please provide a list of the scheduled preventive and predictive maintenance and testing frequencies for critical infrastructure components such as:
  - Electrical systems (infrared testing)
  - Emergency generators
  - UPS devices
  - Switchgear and transformers
  - Automatic transfer switches
  - Static transfer switches
  - Power distribution units (PDUs)
  - Remote power panels or circuit breaker panels
  - Other electrical distribution equipment
  - HVAC system equipment
  - Fire and life safety equipment
- Are your generators tested at load? If yes:
  - How often is this performed and at what load percentage of the full-rated load?
  - How often is end-to-end utility outage testing performed?
  - What items are inspected and recorded during testing?
  - Can the most recent test results be reviewed?
- What are the cleanliness standards for the raised-floor areas?
- How do you manage airborne particulates in the raised-floor areas?
- How do you control and manage installation and maintenance activities in the raised-floor areas and in the mechanical and electrical areas? Is there a documented procedure that can be reviewed?

## Critical Systems Infrastructure Management and Capacity Planning

### Critical equipment:

- Has any of your critical equipment (UPS devices, generators, chillers, etc) exceeded its useful life?
- What is your policy for replacing critical equipment?
- What is your process for evaluating and choosing critical equipment?
- Who are the manufacturers of your critical infrastructure equipment?
- How is your redundant critical equipment configured?
- Is any of your equipment reused or refurbished?
- Are major critical pieces of equipment (such as generators, switchgear, UPS devices, static transfer switches, PDUs and HVAC system components) sourced from the same manufacturer?

### Critical and essential electrical systems:

- How many utility feeds does the facility receive?
- What are the feeder sizes?
- What is the current capacity available from the utility on each feeder?
- Is there reserved capacity for the facility?
- What is the voltage received from the utility service?
- What types of switchgear are used (such as transformers and automatic transfer switches)?
- At what points is transient voltage surge suppression (TVSS) equipment used in the electrical distribution system?
- How many emergency backup generators do you have in place?
- What are the capacities and ratings of the emergency backup generators?
- How are the emergency backup generators configured in terms of redundancy?
- What type of fuel do the emergency backup generators use?
- Are the generators tied to a common bus?
- Do the emergency backup generators use paralleling gear?
- How long does it take for the emergency backup generators to be online and supply the facility with power in the event of a utility outage?
- What is the run time for each emergency backup generator at full load?
- What is the onsite fuel storage capacity?
- In the event of an extended utility interruption, what is the refueling plan? For example, what are the fuel supply sources?
- How many UPS devices service the data center?
- What are the capacities and ratings of the UPS devices in kVA?
- What types of batteries are used?
- What is the battery discharge time at full load?
- How do you manage load capacity on the UPS devices?
- What is the current capacity available on the UPS devices?
- What are the UPS redundancies?
- How many UPS devices can fail without impacting critical load to the data center floor?

- How are multiple UPS devices configured? (Single module or common bus?)
- What is your policy related to UPS battery replacement??
- When was the last time the batteries were replaced?
- Do the UPS devices feed straight to the PDUs or are static transfer switches used to provide multiple source UPS devices to the PDUs?
- Can we review a one-line drawing of your electrical distribution system?
- Can you describe and provide a drawing of the data center's grounding system?
- What was the grounding system tested to?
- Are cabinets and racks individually grounded?

### **Critical HVAC systems:**

- Describe in detail the facility's cooling systems for the data center areas.
- What is the capacity of the cooling system?
- What are the redundancies?
- Is there refrigerant used on the raised-floor areas in any fashion?
- Are cooling towers used? If yes:
  - How many water taps are supplying the facility?
  - Provide a description of the system.
  - What is the backup capacity of make-up water on site?
- Is there leak detection under the raised floors and in the mechanical rooms? If yes:
  - How is it deployed?
  - Is there redundancy in the leak detection devices?
  - Is the leak detection system continuously monitored, and if so, by what means and who is alerted?
- Are there spill containment features in the data center and mechanical plants?
- How is humidity controlled in the raised-floor areas?
- Can we review a drawing of your cooling system?

### **Fire and safety equipment:**

- What types of smoke detection and fire suppression systems are in use?
- Is there an early warning system in use? If yes:
  - What type of system is it?
  - Where are the sampling points located?
  - How is it monitored?
  - What is the process in the event of an early warning alarm?
  - What is the process for identifying the source?
- How often are the fire and safety systems inspected and tested?
- Can we review the maintenance, inspection and testing records?
- Are portable extinguishers used? If yes:
  - Where are they located?
  - How often are they tested and inspected?
  - Is onsite staff trained in portable extinguisher use?
- What are the fire ratings of internal walls throughout the facility?

- Are fire drills conducted on a recurring basis? If yes:
  - What are the process and schedule for fire drills?

#### **Critical systems and equipment monitoring:**

- What types of critical infrastructure monitoring systems are in use?
- What equipment is continually monitored?
- How are monitoring system alerts and alarms disseminated, escalated and resolved?
- Please provide a description of all facility, building and critical systems monitoring systems.
- Are individual electrical branch circuits to equipment racks and cabinets monitored continuously? If yes:
  - Are the monitoring reports available to view?

#### **Infrastructure management standards:**

- What is your cable management policy? How is it enforced?
- How are critical infrastructure equipment and components labeled? (This includes electrical systems including branch circuits, HVAC systems and fire and safety equipment.)
- How are circuit breaker panels and panel schedules managed and maintained?